WASHINGTON STATE DEPARTMENT OF LICENSING

Sample Document: Contracted Plate Search Data Sharing Agreement

This document is an example of a Washington State Department of Licensing data sharing agreement and is intended for reference only.

WASHINGTON STATE DEPARTMENT OF LICENSING

CONTRACTED PLATE SEARCH DATA SHARING AGREEMENT

New Account #

Renewal Account #

Contract

Contract start date	Contract end date	Contract amount
Upon execution by the Parties	1 year	Revenue: Dependent on Usage

Purpose:
This agreement sets out the rules, requirements, and permissions for you (the "Recipient") to use the Department of Licensing's (DOL) Contracted Plate Search (CPS) service.

Authorized use of Data is limited to:

Recipient

Company / agency name	Company trade (doing business as) name
Physical Address	
Mailing Address	

Account Administrator name	Administrator's telephone	Administrator's email address
Business type(s):		Company / agency business web address:

Department of Licensing (DOL)

Department administration	Division
Data Management Office	Director's Office
Address: PO Box 9020 Olympia, WA 98507-9020	

Contract Manager	(Area code) Telephone	Email
Susan Mitchell	(360) 902-3708	dataservices@dol.wa.gov

Attachments

This Agreement consists of the following attachment(s) and exhibits(s) incorporated herein or by reference:

Attachment A, *Privacy and Security Requirements*
Attachment B, *Subscriber Requirements*
Exhibit 1: *Sample notification letter*

This Agreement represents the complete and final understanding between DOL and the Recipient, replacing all previous agreements, written or spoken, regarding the subject matter of this Agreement. This Agreement becomes effective when both Parties sign it. By signing below, both Parties confirm they have read and understand this Agreement and have the legal authority to sign on behalf of their organization.

Recipient Signature	Date	DOL Signature	Date
PRINT Signatory's Name, Title		Name, Title Evelyne Lloyd Assistant Director, Administrative Services Division	
Signatory's e-mail:			

DRAFT

Sample contract

This data sharing agreement (“Agreement”) is made between the Washington State Department of Licensing (“DOL”) and the company or agency (“Recipient”) named on the first page.

"Party" can mean either DOL or Recipient. "Parties" means both DOL and Recipient. Where the Agreement reads “you”, it means Recipient. Where the Agreement reads “we”, it means DOL.

1. PURPOSE
   This Agreement explains DOL’s terms and conditions that give you limited access to, and use of, Confidential Information available through the Contracted Plate Search (CPS) service.

2. LEGAL AUTHORIZATION
   DOL is allowed to share Data, and required to enter into this Agreement, under applicable state and federal laws, including:
   A. Chapters 42.56, 46.12, 46.22, and 46.70 Revised Code of Washington (RCW);
   B. Chapters 308-10, 308-10A, and 308-93 Washington Administrative Code (WAC); and
   C. Federal Driver Privacy Protection Act of 1994 (18 U.S. Code § 2721).

3. KEY DEFINITIONS
   Terms used in the Agreement are defined as follows:

   A. “Account Administrator” (or “Administrator”): The Recipient’s representative responsible for managing the CPS account and the person DOL contacts with any questions or issues pertaining to this Agreement.
   B. “Authorized User” (or “User”): Any person the Recipient allows to access CPS. This includes account managers or Administrators.
   C. “Confidential Information”: CPS information from DOL that must be protected and may not be shared with the public or unauthorized people under Chapter 42.56 RCW or other laws. In this Agreement, it includes vehicle and vessel ownership details and personal information like names and addresses of owners.
   D. “Contracted Plate Search” or “CPS”: The DOL service used to retrieve and show vehicle and vessel owner and title information.
   E. “Data”: All Vehicle and Vessel Record information that DOL provides to the Recipient under this Agreement, including Confidential Information.
   F. “Generative AI”: A technology that can create content, including text, images, audio, or video, when prompted by a user. Generative AI systems learn patterns and relationships from large amounts of data, which enables systems to generate new content that may be similar, but not identical, to the underlying training data.
   G. “Inquiry”: Any search in CPS, whether it returns a record or not.
   H. “Offshoring”: The electronic or hardcopy transmission, accessing, viewing, capturing images, storage, or processing of Confidential Information outside the United States
   I. “Permissible Use”: The use of Confidential Information that is allowed or required by federal or state law (as explained in Section 7).
   J. “Subscriber”: The agency, company, organization, individual, or other entity authorized by state or federal law to use Confidential Information they receive from the Recipient or their Subscriber.

K. “User”: A person that the Administrator sets up in License Express (or a successor system) to access CPS.

L. “Vehicle Record”: Any information in CPS that identifies a specific vehicle or its registered owner.

M. “Vessel Record”: Any information in CPS that identifies a specific vessel or its registered owner.

If there is a difference between these definitions and those in the RCWs or WACs cited in Section 2, Legal Authorization, the RCW or WAC definitions will apply.

SPECIAL TERMS AND CONDITIONS

4. GRANT OF ACCESS
DOL gives you a limited right to access and use Vehicle and Vessel Records under this Agreement. You cannot transfer this right to anyone else. You do not own this Data; DOL remains the owner.

5. AGREEMENT TERM
This Agreement starts when executed by the Parties and ends on DATE unless terminated sooner or extended if both Parties agree in writing. DOL will decide, at is sole discretion, if the Agreement will be extended. It is your responsibility to know when the Agreement approaches the end of its term and to re-apply for an extension or a new agreement. DOL will not send notice or a reminder that the Agreement is reaching the end of its term.

6. SAFEGUARDING DATA
CPS Data contains Confidential Information. You must protect all Confidential Information received under this Agreement from any unauthorized sharing, use, or loss, as explained in Attachment A – *Privacy and Security Requirements*.

7. HOW YOU CAN USE THE DATA (PERMISSIBLE USE)
When entering into this Agreement, you and your Subscribers will only use Data for the specific purposes authorized in Section 7.1 below and as stated on page one (1), and you will not use the information for the purpose of making unsolicited business contact. Any other use of this Data is strictly prohibited. Misuse of the information may lead to immediate termination of this Agreement and result in civil and criminal penalties.

7.1 Authorized Permissible Uses
Your authorized use of CPS Data is limited to:

- Government agencies and their agents:
  - A government agency in the United States or Canada (including courts and law enforcement) carrying out its official duties except as prohibited under RCW 43.17.425.
  - Any private person or business acting on behalf of a government agency.
- Parking violations:
  - A government agency, commercial parking company, or their agents, to notify vehicle owners about unpaid parking violations.
- Insurance activities:
  - An insurance company, insurance support organization, or a self-insured entity (or their agents) for claims investigations, anti-fraud efforts, setting rates, or underwriting policies.

- Towing vehicles:
    - Out-of-state business or its agent to inform owners of vehicles that have been towed or impounded.
- Legal proceedings:
    - In connection with any documented civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency, including investigation in anticipation of litigation with a letter of engagement. This includes serving legal documents and enforcing court orders or judgments.
- Vehicle and Vessel records:
    - Vehicle or Vessel manufacturers, or vehicle and vessel component manufacturers, or their authorized agents, for recall of their own products.
- Written consent:
    - A business seeking a person's information when:
        - The business received written permission from the person before making the Inquiry, and
        - The form used to obtain written permission informs the person the business purpose for obtaining the person's information.

7.2 Data for Training and Testing

You cannot use CPS records solely for training without the prior written consent of the vehicle or vessel owner used in the Inquiry. The form used to obtain consent is valid for thirty (30) days after consent is granted and must be kept on record for five (5) years following the Inquiry.

7.3 Prohibited Uses

A. In compliance with RCW 43.17.425, you and any Subscribers are explicitly prohibited against sharing or using Data for purposes of investigating, enforcing, cooperating with, or assisting in the investigation or enforcement of any federal or state regulation or surveillance programs or any other laws, rules, or policies that target Washington residents solely on the basis of race, religion, immigration, or citizenship status, or national or ethnic origin.

B. In compliance with RCW 7.115.020, you and any Subscribers are explicitly prohibited without limitation against sharing or using Data for purposes of investigating, enforcing, cooperating with, or assisting in the investigation or enforcement of any federal or state programs or any other laws, rules, or policies that target those who are, or were, in receipt of protected health care services that are lawful in the state of Washington.

C. You and Subscribers are explicitly prohibited without limitation against sharing or using Data, including Protected Personal Information, for purposes of creating, maintaining, or operating Generative AI.

8. SUBSCRIBER REQUIREMENTS

If you provide Data to a Subscriber, you must follow all requirements in Attachment B – *Subscriber Requirements*.

9. INSURANCE

Recipient shall maintain self-insurance or commercial insurance as outlined herein. Insurance must be maintained with carriers that are authorized to do business in Washington State and maintain a minimum AM Best rating of A-: VII, or an equivalent rating with a similar rating agency.

A. All insurance must be primary to any other insurance programs afforded to or maintained by DOL or the state of Washington. Recipient waives all rights against DOL and the state of Washington for recovery of damages to the extent that such damages would be covered by general liability or umbrella insurance maintained by Recipient pursuant to this Agreement.
Cyber Liability

B. When the Recipient is receiving Protected Personal Information, the Recipient shall maintain cyber liability insurance with policy amounts as outlined below. A Recipient who has access to funds in Washington State's Self-Insured Liability Pool is deemed to meet this requirement.

   i. The policy amount is based on the number of unique individuals' records containing Protected Personal Information in Recipient's possession on January 1 following the date of receiving data, and every three (3) years thereafter. When DOL previously approved a reduction in policy value, the approval was valid for no more than three (3) years and must be renewed every three (3) years.

   ii. The Recipient's cyber liability insurance policy value is subject to audit to assess if the value accurately corresponds with the number of records held at time of the audit. This insurance shall include coverage for third party claims and losses including with respect to network risks (such as: data Breaches, transmission of virus/malicious code, unauthorized access or criminal use of third party, ID/data theft) and invasion of privacy regardless of the type of media involved in the loss of private information (such as: computers, paper files and records, or voice recorded tapes), covering collection, use, access, etc., of Protected Personal Information, direct liability, as well as contractual liability for violation of privacy policy, civil suits and sublimit for regulatory defense/indemnity for payment of fines and penalties.

Number of Records Containing Protected Personal Information accessed per Contract duration	Policy Value	Policy Value with Mitigations
Greater than one million unique individuals	$100,000,000	$15,000,000
500,001 – 1,000,000 unique individuals	$50,000,000	$7,500,000
250,001 – 500,000 unique individuals	$25,000,000	$3,750,000
100,001 – 250,000 unique individuals	$15,000,000	$2,250,000
50,001 – 100,000 unique individuals	$5,000,000	$1,000,000
5,250 – 50,000 unique individuals	$1,000,000	$1,000,000
1 – 5,249 unique individuals	Policy not required	

10. INVESTIGATIONS
DOL or its agent may without prior notice investigate you for misuse of Confidential Information or compliance with one or more requirements in this Agreement. Like the requirement in Sec. 29,

DOL may require you to provide various records, documents, and other information concerning the investigation.

11. ACCESSING DATA

CPS is designed to provide 24-hour access, but availability cannot be guaranteed. The CPS service may be temporarily inaccessible without prior notice.

To use the CPS service, you must identify and maintain a full-time Administrator as originally designated on page one (1) of this Agreement. The Administrator is responsible for managing all your User accounts under this Agreement. If a User will no longer access Data through your account, the Administrator must immediately remove that User account from the system.

Each User who accesses Data on your behalf must have their own individual account for License Express (or a successor system), DOL's account servicing platform. User accounts cannot be swapped or shared. Each User account must have its own unique username and password. All account activities are recorded in DRIVES to track the information accessed through that account.

The Administrator must actively monitor each User to make sure Data is accessed and used only for official job duties and for the limited uses authorized in this Agreement. The Administrator must immediately remove access for any User who accesses or uses Data in violation of this Agreement or violates any terms of this Agreement. DOL may suspend or end the access of specific Users if DOL believes they are not complying with this Agreement. On-going non-compliance by Users could lead to the termination of this entire Agreement.

12. REPORTING EVENTS

You must notify DOL when you reasonably believe there has been unauthorized access, loss of control, or misuse of Data. This also applies if such events happen with a Subscriber. Report these events to:

A. DOL Help Desk at (360) 902-0111,
B. DOL Compliance Manager at (360) 902-3920, and
C. DOL Event Management at DOLEventMgmt@dol.wa.gov

You must tell DOL about the event before making any public announcement.

13. FEES

The fee for using CPS is $0.04 (four cents) for each Inquiry, even if it returns "no file" or "no record found."

There is a $2.00 (two dollar) fee each time you view a Vehicle or Vessel Record in CPS. Government agencies are exempt from the $2.00 fee.

DOL may increase or decrease fees when required by law and without notice.

14. PAYMENT AND BILLING

Invoices are sent and payments are due monthly unless we agree otherwise in writing.

You must pay invoices within thirty (30) days of the invoice date. Your payment must include your CPS account number and a copy of the invoice. Send payments to:

Department of Licensing, CPS (*your account #*)
P.O. Box 3907
Seattle, WA 98124

DRAFT

Washington State agencies can pay invoices using a journal voucher (JV) or by making an inter-agency payment (IAP) using DOL Statewide Vendor Number SWV0011175-01.

If you don't pay invoices on time, DOL can suspend your access or send your account to a collection agency. DOL might give you advance notice of a suspension or collection but is not obligated to do so.

If your monthly bill is $4.50 (four dollars and fifty cents) or less, DOL may not send a bill. If DOL doesn't send a monthly invoice, the amount due is carried over to the next month; DOL's failure to provide an invoice does not mean you don't have to pay for services, nor does it waive your responsibility to pay the full amount on the next invoice received. If you don't receive an invoice and have concerns, you should contact DOL accounting services at 360-902-7428 immediately.

15. ADDITIONAL RECIPIENT REQUIREMENTS

To keep your access period active, you must:

A. Business License: Keep a current business license for the duration of this Agreement and provide a copy to DOL if requested,

B. User Acknowledgments: Train each User on the requirements in this Agreement. You must have each User read and sign a written acknowledgement that they understand and will fully follow this Agreement. An acceptable version of the form is located at DOL.WA.GOV by searching for Form ID: DSC-425-040 (*DRIVES E-Services Access Appropriate Use Declaration*), and

C. Submit a minimum of 24 Inquiries to the CPS system each calendar year. Accounts that have not submitted a minimum of 24 Inquiries in the past calendar year may be terminated.

D. Respond to requests for audits or assessment results described in Section 29..

E. Attorney/Private Investigator Notification: If you are an attorney or private investigator obtaining Vehicle or Vessel Record Data directly from CPS, you must identify yourself under the Permissible Use menu. In these cases, DOL will mail notification letters to the individuals whose records you review, as required by RCW 46.12.635(4). DOL may charge you for the costs of these mailings.

F. When providing Data to Attorneys/Private Investigators: If you provide Vehicle or Vessel Record Data to a Subscriber that is an attorney or private investigator (and you are not one yourself), you are the disclosing entity under RCW 46.12.635(4). You must send a notification letter to the individual whose records were accessed and shared with an attorney or private investigator. See Exhibit 1 for a sample notice.

   The notification letter must only include:

   i. Information that you disclosed the vehicle or vessel owner's name and address pursuant to a request under RCW 46.12.635,

   ii. The date the disclosure was made, and

   iii. The occupation of the Subscriber.

   You must also provide a copy of the notification letter to DOL's Public Records Office at Notifications@dol.wa.gov.

   When a vehicle or vessel owner presents you with a copy of a valid court order restricting another person from contacting them or their family, you shall provide the vehicle or vessel owner with the name and address of the Subscriber to whom you provided that individual's Vehicle or Vessel Record Data.

GENERAL TERMS AND CONDITIONS

16. AMENDMENTS

This Agreement may only be amended by mutual agreement of the Parties. Such amendments are not binding unless they are in writing and signed by personnel authorized to bind each of the Parties.

Only DOL's Director or designated delegate by writing has the expressed authority to alter, amend, modify, or waive any clause or condition of this Agreement. Furthermore, any alteration, amendment, modification, or waiver of any clause or condition of this Agreement is not effective or binding unless made in writing and signed by DOL's Director or delegate.

17. ASSIGNABILITY

The Recipient may not assign this Agreement or any claim arising under this Agreement.

18. AGREEMENT MANAGEMENT

The Recipient's Account Administrator and DOL's Contract Manager, respectively listed on page one (1), are responsible for all communications and notices pertaining to this Agreement. All such communications and notices are to be made between the respective managers unless alternative personnel are established for specific purposes. The use of email, to the most current email address on file for the other Party, is an acceptable form of providing notice for all purposes in this Agreement.

The Recipient is required to notify DOL in writing within three (3) business days of changes to: business name, ownership, business address, phone number, email address, or Account Administrator and their contact information.

19. DATA DISPOSITION CERTIFICATION

The Recipient, upon the termination, expiration, or cancellation of this Agreement, must dispose of all Data and execute a written certification attesting to such disposal and the method used. The certification must be in the words of the Recipient. DOL does not provide a form for this purpose.

You must provide the legal basis in writing to DOL when any Data is retained for more than 30 days following termination, expiration, or cancellation of this Agreement.

20. DISPUTES

The Parties agree that time is of the essence in resolving disputes.

When a dispute concerning a question of fact arises between DOL and the Recipient and it cannot be resolved, either Party may request a dispute hearing with DOL's Contracts Office. This is a requisite prior to seeking any court action to resolve the dispute.

When a dispute arises between state agencies, agencies shall employ every effort to resolve the dispute themselves without resorting to litigation. These efforts shall involve alternative dispute resolution methods. If a dispute cannot be resolved by the agencies involved, any one of the disputing agencies may request the governor to assist in the resolution of the dispute. RCW 43.17.330.

21. GOVERNANCE

This Agreement is to be construed and interpreted in accordance with the laws of the state of Washington and the venue of any action brought hereunder will be in the Superior Court for Thurston County.

DRAFT

In the event of an inconsistency in this Agreement, unless otherwise provided, the inconsistency shall be resolved by giving precedence in the following order:

A. Applicable federal and Washington State laws, and regulations;
B. Terms and conditions of this Agreement;
C. Attachment A – *Privacy and Security Requirements*
D. Attachment B – *Subscriber Requirements*;

22. INDEMNIFICATION

To the extent allowed by law, the Recipient shall defend, indemnify, protect and hold harmless DOL from and against all claims, suits, actions and all associated costs arising from any negligent or intentional acts or omissions of the Recipient, or any Subscribers who received the Data from the Recipient, during the performance of this Agreement. This includes all matters related to the data security and permissible uses of the Data.

23. INDEPENDENT CAPACITY

The scope of this Agreement maintains each Party's independent status as a self-governed entity, and nothing herein may be deemed as causing the Recipient, or any employee, personnel, or agent of the Recipient to be considered as the employee, agent, or subcontractor of DOL.

24. INTEGRITY OF DATA

Vehicle and Vessel Records are only presumed accurate at the moment viewed and are updated in real time. DOL shall not be liable for any delays in furnishing refreshed Data, nor shall DOL be liable for any errors in the Data.

25. RECIPIENT LEGAL COMPLIANCE STANDARDS

The Recipient, as a Party under this Agreement with DOL, must comply with all applicable local, state, and federal laws, rules and regulations. Such compliance minimally includes without limitation, all applicable licensing requirements of the state of Washington, all civil rights and non-discrimination laws, the Americans with Disabilities Act (ADA) of 1990, all federal and state employment laws, the Protecting Americans' Data from Foreign Adversaries Act of 2024, and the Data Security Program under federal Executive Order 14117. Failure to comply with this provision may be grounds for termination of this Agreement regardless of effect it may have on the subject matter of this Agreement.

26. NON-DISCRIMINATION

A. Nondiscrimination Requirement
During the term of this Agreement, the Recipient, including any Subscriber, shall not discriminate on the basis enumerated at RCW 49.60.530(3). In addition, the Recipient, including any Subscriber, shall give written notice of this nondiscrimination requirement to any labor organizations with which the Recipient, or Subscriber, has a collective bargaining or other agreement.

B. Obligation to Cooperate
The Recipient, including any Subscriber, shall cooperate and comply with any Washington state agency investigation regarding any allegation that the Recipient, including any Subscriber, has engaged in discrimination prohibited by this Agreement pursuant to RCW 49.60.530(3).

C. Default
Notwithstanding any provision to the contrary, DOL may suspend the Recipient, including

any Subscriber, upon notice of a failure to participate and cooperate with any state agency investigation into alleged discrimination prohibited by this Agreement, pursuant to RCW 49.60.530(3). Any such suspension will remain in place until DOL receives notification that the Recipient, including any Subscriber, is cooperating with the investigating state agency. In the event the Recipient, or Subscriber, is determined to have engaged in discrimination identified at RCW 49.60.530(3), DOL may terminate this Agreement in whole or in part, and the Recipient, Subscriber, or both, may be referred for debarment as provided in RCW 39.26.200. The Recipient or Subscriber may be given a reasonable time to cure this noncompliance, including implementing conditions consistent with any court-ordered injunctive relief or settlement agreement.

D. Remedies for Breach
Notwithstanding any provision to the contrary, in the event of Agreement termination or suspension for engaging in discrimination, the Recipient, Subscriber, or both, shall be liable for contract damages as authorized by law including, but not limited to, any cost difference between the original contract and the replacement or cover contract and all administrative costs directly related to the replacement contract, which damages are distinct from any penalties imposed under chapter 49.60, RCW. DOL shall have the right to deduct from any monies due to the Recipient or Subscriber, or that thereafter become due, an amount for damages the Recipient or Subscriber will owe DOL for default under this provision.

27. PUBLIC REQUESTS FOR INFORMATION
All records, including your application, this Agreement, and search history are available to the public under chapter 42.56 RCW, *Public Records Act*.

If the Recipient is a governmental entity, then to the extent consistent with chapter 42.56 RCW, the Recipient will maintain the confidentiality of all Confidential Information provided under this Agreement. If a public records request or subpoena is made for Confidential Information, Recipient will withhold the information, notify DOL of the request, provide DOL with a copy of the request, and allow DOL adequate time to review the request and obtain a court injunction if necessary.

28. PUBLICITY & MEDIA
The Recipient may not engage in any publicity or media, relative to the subject matter of this Agreement, where DOL's name is included, or may be reasonably be implied, unless the Recipient first provides copy of such publicity and media to DOL, and DOL approves and permits the same. If DOL approves any advertising and publicity matter, DOL reserves the right to add a disclaimer and/or rescind its approval at a later date.

29. RECORDS ACCESS AND INSPECTIONS
The Recipient, at the request of DOL, must provide, access to all records retained in connection with this Agreement. This is to include for a period no less than the past five (5) years, and without limitation: all Data shared with a Subscriber and the permissible use of such Data and the forms used to obtain written permission. Records must be made available for DOL to inspect and review in non-redacted form regardless of any claim of privilege or confidentiality. DOL may request copies at no additional cost to DOL.

The Recipient must carry forward the requirements of this section to all Subscriber contracts, giving DOL the right to access, review, inspect, and copy the Subscriber's records in connection with your written agreement. The Recipient may not enter into any non-disclosure agreements that directly or indirectly prevents DOL from reviewing any Subscriber's records under this

Agreement.

30. AUDITS AND SELF-ASSESSMENT

In addition to the right to conduct investigations (Sec. 8) and right of access to records (Sec. 28), DOL or its agent may audit you for compliance with this Agreement. The scope and scale of each audit will be in proportion to the volume of records you accessed through CPS, or the cumulative number of records you accessed through all data sharing agreements with DOL.

You will be audited for compliance with the requirements in Attachment A - *Privacy and Security Requirements*, the Special Terms and Conditions, and General Terms and Conditions in this Agreement when:

A. Non-governmental entities: your account is invoiced for more than $10,000.00 in a calendar year, or
B. Governmental entities: your account exceeds 5,000 record views in a calendar year.

You will receive advance notice of each audit along with a request for information that is required to prepare and conduct the audit. You are required to cooperate with all audit requests in a timely manner. Cost of audits, including DOL or its agent's labor, will be at the expense of the Recipient. DOL will provide a cost estimate upon request.

At the completion of the audit, you will receive a draft report and be given an opportunity to provide a response to all findings and conclusions. When the final audit report contains exceptions, DOL will work with you on a corrective action plan for any exceptions.

In addition to DOL conducting Audits, the Recipient has the continuing obligation to perform a self-assessment of its compliance with Attachment A - *Privacy and Security Requirements* and Attachment B – *Subscriber Requirements*. The self-assessment must be performed on an annual basis for every one-year interval period of this Agreement – performed at the end of each period. Upon DOL's request, the Recipient must use information gathered through each self-assessment to confirm in writing to DOL, not later than 30 days after DOL requests the assessment results, whether Recipient is in compliance with the requirements set forth in Attachment A - *Privacy and Security Requirements* and Attachment B - *Subscriber Requirements*.

31. RECORDS MAINTENANCE

The Recipient shall maintain all records relating to this Agreement, including all service and account records, all notifications to vehicle or vessel owners that their information was shared with an attorney or private investigator, all compliance records, Permissible Use documentation, investigation records related to the release and use of Confidential Information, and all correspondence and legal records related to Subscribers for a period of at least six (6) years beyond the term of this Agreement. Records do not include Data, which must be disposed of in accordance with Section 18.

If any litigation or audit is started before the expiration of the six-year period, the records must be retained until all litigation, claims, or audit findings involving the records have been resolved including any appeals and remands.

32. SEVERABILITY

If any term or condition of this Agreement is held invalid, the remainder of the Agreement remains valid and in full force and effect.

33. SURVIVORSHIP

The terms, conditions and warranties contained in this Agreement concerning Permissible Use of

Data, Privacy and Security Requirements, Subscriber Requirements, record retention, and Data destruction, survive the completion of the performance, cancellation or termination of this Agreement until the Recipient provides DOL an attestation of Data disposal.

34. TERMINATION

Termination of this Agreement may be made as set forth below. DOL may at its sole discretion choose to suspend instead of terminating this Agreement on the terms and grounds set forth below for termination. DOL has the authority to terminate any account suspended for more than 90 days.

A. Unilateral Termination by Recipient

The Recipient may terminate this Agreement at any time and for any reason upon providing written notice to DOL. If at the time of termination, the Recipient was not in compliance with this Agreement, DOL may refuse future agreements.

B. Administrative Terminations

If DOL's authority to actively engage in this Agreement is suspended or terminated, such a termination or suspension will automatically cause a termination or suspension of this Agreement.

Additionally, if DOL, as a state agency, determines that the continuation of this Agreement no longer conforms to DOL's policy, and/or is no longer in the best interests of DOL or the state of Washington, DOL may terminate this Agreement for convenience by giving written notice to Recipient at least fifteen (15) business days before the effective date of termination. Administrative terminations are without cause.

C. Termination for Cause

DOL may terminate this Agreement or suspend the access period if the Recipient or a Subscriber violates a term, condition, or requirement of this Agreement. DOL has sole discretion on whether the Recipient or Subscriber's non-compliance is cause for an immediate termination or suspension, and whether the Recipient or Subscriber should be given a cure process to correct the non-compliance.

For any determination of non-compliance, DOL must provide the Recipient with a written statement identifying the full nature of the Recipient's breach and justifying DOL's reasoning for seeking immediate suspension, termination, or a cure process. DOL may suspend the access period to Data during a cure process. If DOL allows for a cure process, the Parties will work together to establish the process and timeline. The agreed-upon cure process will be put in writing and acknowledged by both Parties. If Parties cannot mutually determine a cure process, or if the Recipient does not substantially complete the cure process within the stated timelines, DOL then has the right to elevate the matter to a final termination.

35. REMEDIES NOT EXCLUSIVE

The rights and remedies of the Parties as provided in this Agreement, are not exclusive and are in addition to any other rights and legal remedies provided by law, including without limitation, the right to receive financial reimbursement for any incurred damages.

36. WAIVER

A failure by either Party to exercise its rights under this Agreement shall not preclude that Party from subsequent exercise of such rights and shall not constitute a waiver of any other rights under this Agreement unless stated to be such in a writing signed by an authorized representative of the Party and attached to the original Agreement.

ATTACHMENT A – PRIVACY AND SECURITY REQUIREMENTS

The following requirements serve to protect Confidential Information from unauthorized access and misuse. They represent best practices for all business entities.

1. PRIVACY REQUIREMENTS

You must have a privacy framework that guides how you handle confidential information. At a minimum, your framework must include ways to identify and manage privacy risks, including the following:

1.1 Privacy Policy
You must have an internal privacy policy that:

a. Informs employees that data is managed as an asset of your organization and explains how data will be protected, and
b. Sets the expectation that all staff will secure, use, and dispose of Data in line with your privacy and security practices and this Agreement.

1.2 Training
You must train your staff, including contractors, who have access to Data on your privacy policy.

1.3 Privacy Notice
You must have a privacy notice that informs the public how you collect, share, use, reveal, and manage Data.

1.4 Incident Response Plan
You must have a plan to respond to any incident or breach involving Data. At a minimum, this plan must include:

a. Procedures you use to prepare for, detect, respond to, and recover from incidents and breaches.
b. Notification to DOL
c. Notification in accordance with chapter 19.255 RCW or RCW 42.56.590.

DOL may update these Privacy Requirements as state policy or law requires.

2. DATA SECURITY REQUIREMENTS – RECIPIENTS SUBJECT TO WATECH SECURITY POLICIES

2.1 WaTech Guidance
You must follow Washington Technology Solutions (WaTech) or equivalent guidance on securing information technology assets as provided in WaTech IT Security Policies and Standards (SEC series).

2.2 IT Security Assessment
In addition to the audit requirements in this Agreement, you must provide DOL with evidence that you conducted a recent IT Security Assessment, specifically for the systems that store, process, or send Data. See Risk Assessment Standard, SEC-11-01-S.

2.3 Data Minimization
You must have a policy for how long you keep Data. You must only keep Data for as long as needed to fulfill the purpose for which you obtained it, and/or in line with your agency's record

DRAFT

retention policies.

2.4 Data and Media Sanitization

You must have a data and media sanitization policy that aligns with the Media Sanitization and Disposal Standard, SEC-04-02-S. This includes:

a. "Clearing" Data from media once it has met the retention policy required in Section 2.3, "Data Minimization."
b. "Purging" Data from media when media is reused for purposes within your organization but will not store Confidential Information or PPI.
c. "Destroying" media that stored Data when the media will not be reused by your organization.

Unless required by law, you must provide a certificate of Clearing, Purging, or Destroying media storing Data within thirty (30) days of:

a. Written request by DOL, or
b. Termination of this Agreement.

2. DATA SECURITY REQUIREMENTS – RECIPIENTS NOT SUBJECT TO WATECH SECURITY POLICIES

All Confidential Information in electronic form must be secured as follows:

You must protect Confidential information using administrative, technical, and physical measures that meet commonly accepted standards for your industry and best practices, including those set by Washington Technology Solutions (WaTech). Examples of commonly acceptable cybersecurity standards and best practices include:

a. ISO 27002
b. PCI-DSS
c. NIST 800 series
d. WaTech IT Security Policies and Standards (SEC series)

DOL will audit based on WaTech's IT Security Policies and Standards if you do not have an industry standard that DOL finds acceptable for securing electronic information.

You must meet the following minimum requirements for securing Confidential Information. Your controls for each topic must align with the industry standard you choose, or as otherwise required by DOL below:

2.1 Network Security

You must:

a. Use a network firewall that protects relevant systems from untrusted networks.
b. Have an intrusion detection system or methods that find and/or prevent unauthorized access on the network.
c. Perform quarterly vulnerability assessments and annual penetration tests.

2.2 Access Security

You must have active user authentication that, at a minimum:

a. Prohibits the sharing of user authentication credentials, such as usernames, passwords, or any other form of identification, to access systems,

b. Establishes a maximum of five failed login attempts and lock the account for a minimum of 15 minutes or until reset by an administrator,
c. Requires a password reset as soon as a password/passphrase is suspected to have been compromised,
d. Passwords with fewer than 15 characters in length may be used for a maximum of 120-days, or a 365-day expiration for passwords having a minimum of 15 characters in length, and
e. Prohibits the use of generic and shared accounts.

2.3 Application Security

a. You must ensure that relevant systems receive software updates, patches, and bug fixes. The software must always be secure from known vulnerabilities ranked “High” or above.
b. All web applications must meet at least the security controls generally described in either:
    i. The Open Web Application Security Project Top Ten (OWASP Top 10), or
    ii. The CWE/SANS Top 25 Most Dangerous Software Errors.

2.4 Computer Security

You must:

a. Keep relevant operating systems and software updated with patches at least monthly, so they remain secure from known vulnerabilities ranked “High” or above.
b. Have an active anti-malware solution with signatures updated at least weekly.

2.5 Data Storage

a. You must keep a list of all computer systems that store, process, or send Confidential Information.
b. Confidential Information cannot be processed on or transferred to any removable portable storage device at any time.

Note: Laptop/tablet computing devices are not considered portable storage devices when they have end-point encryption installed.

2.6 Electronic Data Transmission

You must secure all internal and external electronic transmissions of Confidential Information with strong encryption.

2.7 Data at Rest

You must encrypt Confidential Information while it is stored with strong encryption.

2.8 Data Minimization

You must have a policy for how long you keep Confidential Information. You must only keep Confidential Information for as long as needed to fulfill the Permissible Use for which you obtained it, as well as any legal requirements to keep the record for a minimum period.

2.9 Data and Media Sanitization

a. You must have a policy for cleaning and disposing of data and media that follows current NIST SP 800-88 guidelines and definitions. This includes:
    i. “Clear” or “Clearing”
    ii. “Purge” or “Purging”
    iii. “Destroy” or “Destroying”
b. Unless specifically required by law, you must provide one or more certificates confirming the Clearing, Purging, or Destroying of media storing Confidential Information within thirty

DRAFT

(30) days of:
   i. A written request by DOL, or
   ii. The termination of this Agreement.

3. DATA SECURITY REQUIREMENTS – HARD COPY RECORDS

All Confidential Information in hard copy (printed) form must be secured as follows:

3.1 Hard Copy Storage

Printed copies must be stored in locked containers or storage areas when not in use by authorized people. Examples include a physically secure workspace, locked cabinets, or vaults. Hard copy documents must never be unattended or in areas accessible to the public.

3.2 Hard Copy Transportation

Hard copy documents containing Confidential Information taken outside a secure area must be carried by an authorized person, or a trusted courier service that provides tracking. You must keep records for all transported hard copies showing who (person(s)/courier(s)) was responsible for the transportation, including who received it.

4. DATA SECURITY REQUIREMENTS – OFFSHORING

4.1 Offshoring – Electronic Records

You must keep the primary, backup, disaster recovery, and other sites for processing or storing Confidential Information only in the United States.

You may not, without advance written approval from DOL:

a. Directly or indirectly (including through Subrecipients), send Confidential Information outside the United States.
b. Allow access to Confidential Information from outside the United States.

4.2 Offshoring – Hard Copy

a. You must keep all hard copies containing Confidential Information at locations in the United States.
b. You may not directly or indirectly (including through Subrecipients) transport any Confidential Information outside the United States unless you have advance written approval from DOL.

5. PERMISSIBLE USE REQUIREMENTS

5.1 Data Use and Training

You must create and follow written policies to ensure Confidential Information is only used as allowed in this Agreement. At a minimum, these policies must include training for all staff who access Confidential Information. Training must cover:

a. The allowed uses of Confidential Information as authorized in the Agreement.
b. Limitations on how Confidential Information can be used, prohibiting its use for anything other than what is allowed in the Agreement.
c. Penalties for breaking rules about Confidential Information.
d. How to identify and report an Incident or Breach of Confidential Information.

5.2 Permissible Use Verification

You must confirm that your use and sharing of Confidential Information follows the allowed uses established in this Agreement.

DRAFT

5.3 Monitoring Personnel

You must use administrative, technical, and physical methods to monitor your staff to ensure they use Confidential Information only as authorized in this Agreement across all business practices. These methods must cover monitoring access to and use of Confidential Information.

DRAFT

ATTACHMENT B – SUBSCRIBER REQUIREMENTS

You must apply these Subscriber Requirements to any Subscriber. Confidential Information may only be shared with a Subscriber that qualifies to have the same Permissible Use DOL granted to you. The Subscriber is prohibited from using the Confidential Information for any other purpose. Subscribers may pass Confidential Information onto their Subscribers that are authorized to use the information under state or federal law.

1. You must have a written agreement with Subscribers

   The agreement must include:
   a. A clear statement what the Subscriber is allowed to do with the Confidential Information, and that any other use is prohibited.
   b. A statement that DOL is the sole owner of Data.
   c. A requirement that the Subscriber take all reasonable security procedures necessary to prevent the unauthorized disclosure and misuse of Confidential Information.
   d. A requirement that you be notified if the Subscriber has any type of data breach.
   e. A requirement that you will audit the Subscriber to make sure they are in compliance with your agreement.
   f. A statement that the Subscriber is prohibited from Offshoring Data.

2. You must screen your Subscribers

   Your Subscriber must be a legitimate business that is legally allowed to use the Confidential Information.

3. You must keep a list of all current Subscribers and provide the list to DOL upon DOL's request.

4. Sharing Confidential Information with Attorneys or Private Investigators
   a. When you disclose information to a Subscriber that is either an attorney or private investigator, you must send a notice to the vehicle or vessel owner that tells the owner:
      a. Their name and address were shared under the authority of RCW 46.12.635 (4),
      b. The date the disclosure was made, and
      c. The occupation of the Subscriber that requested the information.
   b. If your Subscriber provides owner information to their Subscriber that is a lawyer or private investigator, they must send the notification letter.

   All notification letters must follow the sample provided in Exhibit 1: Sample Notice.

5. You are Responsible for your Subscribers
   a. Auditing your Subscribers allows you to reduce the risk that they are misusing Data.
   b. DOL will investigate when they suspect a Subscriber is misusing Data.
   c. DOL may want you to suspend a Subscriber from accessing Data. DOL will tell you to stop sharing data with a specific Subscriber and you must suspend their access. DOL should provide you with an explanation for suspending the Subscribers access period, but it is not guaranteed.
   d. You risk having this Agreement terminated if Subscriber misuse is a recurring event, whether it be a single Subscriber or multiple Subscribers.

DRAFT

EXHIBIT 1 – SAMPLE NOTIFICATION LETTER

Note: Recipient must not incorporate or use DOL's letterhead, seal, or logo in the notice.

Date

Name
Mailing address
City, state, zip

VEHICLE VESSEL RECORD DISCLOSURE NOTICE

This provides notice that your name, address, and vehicle/vessel registration information were recently disclosed pursuant to a request under Revised Code of Washington (RCW) 46.12.635. No action is required of you.

If you have both a physical and mailing address on file with the Department of Licensing, only the mailing address was disclosed.

The disclosure of your information was made on [*month day year*]. The information was disclosed to [*an attorney* or *a private investigator*].

This notice is required under RCW 46.12.635.

DRAFT